

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF

**REAR ADMIRAL DAVID S. BELZ
ASSISTANT COMMANDANT FOR OPERATIONS
U.S. COAST GUARD**

**JAYSON AHERN
ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS,
CUSTOMS AND BORDER PROTECTION**

**TOM BLANK
ASSISTANT ADMINISTRATOR OF TRANSPORTATION SECURITY
POLICY**

**CHARLES STALLWORTH
DIRECTOR, AIR AND MARINE OPERATIONS
IMMIGRATION AND CUSTOMS ENFORCEMENT**

ON THE

**MARITIME SECURITY OPERATIONS WITHIN
THE DEPARTMENT OF HOMELAND SECURITY**

BEFORE THE

**SELECT COMMITTEE ON HOMELAND SECURITY
U. S. HOUSE OF REPRESENTATIVES**

MAY 05, 2004

MARITIME SECURITY OPERATIONS WITHIN
THE DEPARTMENT OF HOMELAND SECURITY
BEFORE THE
SELECT COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES
MAY 5, 2004

Good afternoon Mr. Chairman and distinguished Members of the Committee. It is our pleasure to be here today to testify on maritime security operations within the Department of Homeland Security.

Prior to the attacks of September 11, 2001, the primary focus within the maritime domain had been on safety, the environment, vessel traffic management, and law enforcement. Most national and international efforts revolved around the safe and efficient movement of waterborne commerce, the interdiction of narcotics and illegal migrants, and trade compliance. In the post September 11, 2001 era, we recognize that any maritime conveyance could transport or constitute a security threat. In this new environment, components of DHS involved in maritime security have added to their existing efforts by deploying resources to identify such threats, deter and/or prevent attacks, respond, and recover from any maritime security incidents.

The challenge is significant:

- Over 95% of overseas trade enters through U.S. seaports;
- Our seaports account for 2 billion tons and \$800 billion of domestic and international freight each year;
- Each year approximately 9 million sea containers enter the U.S. via our seaports;
- 26,000 miles of commercially navigable waterways serving 361 U.S. ports;
- Strategic military value of many ports and waterways;
- Seaborne shipment of approximately 3.3 billion barrels of oil each year;
- 6 million cruise ship passengers travel each year from U.S. ports;
- Ferry systems transport 180 million passengers annually;
- Waterways support 110,000 commercial fishing vessels, contributing \$111 billion to state economies;
- 78 million Americans engaged in recreational boating;
- Some 8,100 foreign vessels making 50,000 U.S. port calls each year; and
- Domestic and international trade is expected to double in next 20 years.
- Existing maritime smuggling networks can facilitate the illicit movement of people and equipment into the U.S., particularly as legal points of entry are hardened.

While this Committee certainly needs no reminder, it is plainly evident that a terrorist incident against our marine transportation system could have a disastrous impact on global shipping, international trade, and the world economy.

The world's oceans are global thoroughfares. A cooperative international approach involving partnerships of nations, navies, coast guards, law-enforcement agencies, and commercial shipping interests is essential – with all parties acting collaboratively to confront broadly defined threats to our common and interdependent maritime security. The Department of Homeland Security (DHS) recently marked its first anniversary and we are happy to report that operating with other federal agencies sharing a common DHS mission perspective provides new benefits to our nation's security daily.

We are committed to working with our partner agencies as one team engaged in one fight, and truly believe having one Department responsible for homeland security has made America more secure today. Events in Haiti a few months ago provide an example of the leaps forward we are taking with regard to interagency cooperation. Under the direction of the Secretary of Homeland Security, the Homeland Security Task Force – Southeast was stood-up as part of OPERATION ABLE SENTRY. The Coast Guard (CG) led task force was comprised of many agencies chartered to plan, prepare, and conduct migrant interdiction operations in the vicinity of Haiti due to the escalation of violence in that country and the threat of a mass exodus of undocumented migrants. Within the first days of interdiction operations, the task force demonstrated impressive agility and synergy:

- CG cutters, with Citizenship and Immigration Service (CIS) asylum pre-screening officers and interpreters aboard, interdicted 18 Haitian vessels with 1,076 undocumented migrants;
- CG and Immigration and Customs Enforcement (ICE) Air and Marine Operations (AMO) aircraft patrolled the skies throughout the operating area; and CG, ICE, and Customs and Border Protection (CBP) conducted coordinated patrols off the Florida coast;
- CG and ICE conducted a coordinated boarding of a boat suspected of being hijacked off the coast of Miami; and
- Federal Emergency Management Agency (FEMA) also deployed three Information and Planning Specialists to the task force in support of contingency planning.

With our federal government's Awareness, Prevention, Protection, Response and Recovery capabilities now under one roof, in one department, the level of communication and cooperation among the sister agencies of CG, TSA, ICE and CBP is stronger than ever. Under DHS and BTS leadership, CBP, TSA and CG are working together to support efforts to implement the Maritime Transportation Security Act (MTSA) through interagency working groups addressing cargo security standards, port security assessments, international port security and the development of the National Maritime Security Plan.

Additionally, the sister agencies within DHS are forging strong relationships in regards to acquisition management. DHS has established a Strategic Sourcing Group and a series of commodity councils. The purpose of the Strategic Sourcing Group is to assist in the successful development, deployment and maintenance of sourcing strategies to enhance DHS acquisition system and ensure commodities are acquired in the most efficient and effective manner. The purpose of each council is to develop long-term strategies for acquiring a commodity across the department. Some councils that exist include Weapons & Ammunition, Boats, Aviation, Training, Facilities, and Information Technology.

Maritime Strategy for Homeland Security

Since 9/11, Secretary Ridge and all DHS components have worked hard to achieve DHS's strategic goals of Awareness, Prevention, Protection, Response and Recovery. These strategy elements guide all that we do and likewise represent key pillars of the maritime homeland security strategy:

DHS Strategic Goal

Awareness

Maritime Strategy for Homeland Security

Enhance Maritime Domain Awareness (MDA)

Prevention

Build and administer an effective maritime security regime – both domestically and internationally

Protection

Increase military and civil operational presence in ports, coastal areas, and beyond – leverage State, Local and Private Sector assets as well

Response

Improve our response posture in the event a security incident occurs

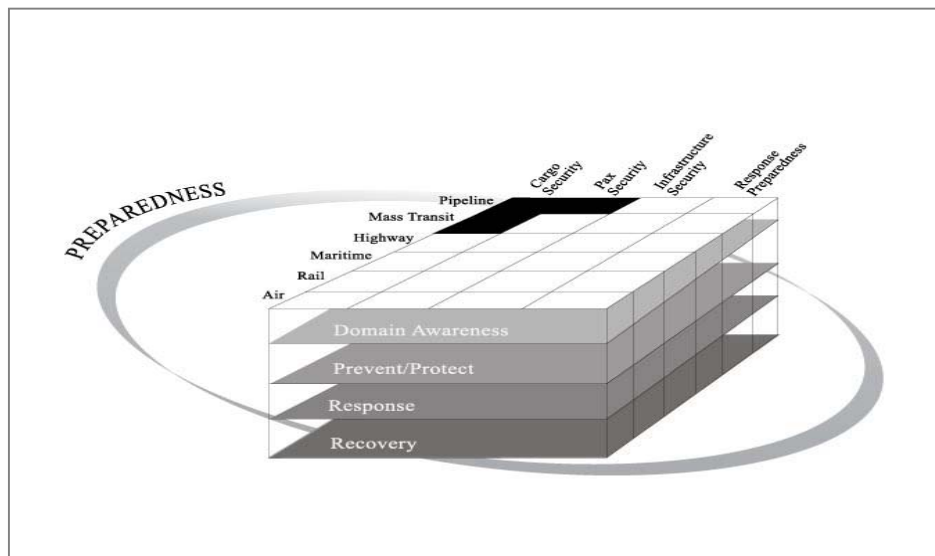
Recovery

Lead efforts to restore services after acts of terrorism, natural disasters or other emergencies

DHS, pursuant to HSPD-7, is in the process of developing a National Critical Infrastructure Plan that will identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. This plan will be comprised of Sector Specific Plans (SSPs), and TSA has been assigned primary responsibility for developing the transportation specific SSP. The Transportation SSP will discuss how federal and private-sector stakeholders will communicate and work together; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how R&D will be prioritized in the sector. In the Transportation Sector, the SSP will further these efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors.

In developing the transportation SSP, TSA is working under BTS guidance and with partners in the U.S. Coast Guard, other BTS component agencies and the Department of Transportation (DOT) and its modal administrations. DHS will build on the foundation of the SSP to provide overall operational planning guidance on transportation security. The expanded SSP will ensure that modal security plans are integrated into an effective concept of operations for management of the transportation sector's security.

Given its unique blend of authorities, capabilities, competencies and partnerships (domestic and international), the CG has been charged with taking the lead on the development and implementation of a comprehensive Maritime Strategy for Homeland Security. The CG's *Maritime Strategy for Homeland Security* supports the President's *National Security Strategy of the United States of America*, the *National Strategy for Homeland Security*, and the *Homeland Security Presidential Directive 7 (HSPD-7)* and is responsive to near-term needs while maintaining a strategic outlook on the threats and opportunities of the future. The maritime strategy is built upon a layered defense; a time-proven means to enhance security in U.S. ports and waterways while concurrently facilitating the smooth flow of commerce. The collective result of our efforts is aimed at managing and reducing maritime security risks.



Below is an update on the Department's recent accomplishments in pursuit of each element of the maritime strategy with a particular focus on the joint and individual efforts of the CG, TSA ICE/AMO and CBP.

Awareness - Enhance Maritime Domain Awareness (MDA)

The core of our MDA efforts revolve around the development and employment of accurate information, intelligence, and targeting of vessels, cargo, crews and passengers – and extending this well beyond our traditional maritime boundaries. All DHS components are working hard to provide an effectively layered defense through collaborative efforts with our international partners to counter and manage security risks long before they reach a U.S. port – when effectively deploying countermeasures becomes more difficult.

The goal is to know the difference between friend and foe, so that legitimate commerce can move through our coastal and port areas unimpeded while we interdict contraband cargo and illegal activities of all types at sea before it becomes a threat on our shores. The key to achieving this comprehensive domain awareness is our ability as a department to obtain, synthesize and analyze the context around the movement of goods and people. We are taking an interagency approach, leveraging information technology, multiple information sources and actively involving the private sector. Our ability to achieve better MDA will allow us to better focus our protection and response efforts on those trade transactions, individuals, and activities of interest. A synopsis of our collective efforts is provided below:

- The CG is leading the interagency and joint Service effort to develop a comprehensive national MDA plan and system architecture.
- As directed by MTSA, the CG established an International Port Security Program (IPSP) that is currently working in concert with CBP, TSA and other Federal agencies to identify foreign ports identified as posing a potential security risk to international maritime transportation. TSA and CBP have provided extensive assistance in developing this program by sharing lessons learned and best practices from TSA's Civil Aviation Security Liaison Officer (CASLO) program and CBP's Container Security Initiative. The IPSP will begin visiting selected foreign ports in July 2004 to measure the degree of rigor with which foreign countries are administering the International Maritime Organization's (IMO) International Ship & Port Facility Security Code (ISPS).

- The CG is researching technologies and systems that are able to track vessels entering, departing or transiting U.S. waters and track vessels bound for the U.S. from overseas locations. The CG is currently working with IMO to develop functional and technical requirements for long-range tracking out to 2,000 nautical miles (approximate distance from shore a vessel owner must transmit their 96-hour notice of arrival, based on typical speed of advance). The U.S. will discuss and attempt to forward an amendment that has been proposed to IMO for this initiative in committee meetings over the next two months.
- The CG is establishing a network for receiving and distributing Automatic Identification System (AIS) reports (position, course, speed, cargo, etc.) from ships using existing Vessel Traffic Services in nine of our nation's ports, waterways, and coastal areas. This initiative will progress to the other strategically significant U.S. seaports, and ultimately extend to nationwide coverage.
- The CG Intelligence Coordination Center, co-located with the Office of Naval Intelligence at the National Maritime Intelligence Center in Suitland, Maryland, established COASTWATCH. Through this process, notice of arrival reports from the National Vessel Movement Center are analyzed using law enforcement and intelligence information and vessels of interest are identified so that Coast Guard and other agencies can appropriately respond to board those vessels before they reach port, if necessary. The Coast Guard and CBP have exchanged personnel to enhance data sharing between the CG Intelligence Coordination Center's COASTWATCH (which gathers and analyzes information on ship notice of arrival reports on vessels, people, and certain dangerous cargoes approaching U.S. ports) and CBP's National Targeting Center (cargo tracking) process.
- CBP's National Targeting Center (NTC) is a 24x7 operation that supports the enforcement and regulatory missions of various agencies through a network of liaisons, which includes the TSA, CG, Department of Energy, and members of the intelligence community. CBP Officers and Field Analysis Specialists that are experts in passenger and cargo targeting for air, sea, and land operations in the inbound and outbound environments primarily staff NTC. The NTC staff develops tactical targets from raw intelligence in support of the CBP mission to detect and prevent terrorists and terrorist weapons from entering the United States. NTC also supports CBP field elements, including Container Security Initiative personnel stationed in countries throughout the world, with additional research assets for passenger and cargo examinations. NTC personnel are also currently engaged in the support of intradepartmental and interagency anti-terrorist operations, while simultaneously providing support to CBP targeting programs, policies, and initiatives. One example of CBP's commitment to collaborative targeting efforts is the Food and Drug Administration Prior Notice Center located at the NTC and operational since December 11, 2003. There, CBP and Food and Drug Administration personnel conduct joint targeting on a round the clock basis in support of the Bio-Terrorism Act.
- CBP is conducting national targeting and using automated targeting tools to screen advance information and other data to identify high-risk shipments. As a key component of the DHS maritime security strategy, CBP's Automated Targeting System (ATS) is a critical tool for performing transactional risk assessments and evaluating potential national security risks posed by sea, air, truck, and rail cargo.

- ICE/AMO is reviewing an upgrade to the Tethered Aerostat Radar System (TARS) to provide an ocean surface track capability along the Southern coast. Airspace data gathered by TARS is integrated within the national surveillance picture at the Air and Marine Operations Center in Riverside, California which provides that data to NORAD, the U.S. Secret Service Operations Center and the National Capital Region Coordination Center.
- ICE/AMO P-3 aircraft have provided the ability to conduct hull-checks on incoming commercial vessels 200 nautical miles from the ports to assist CG prioritization and identification of in-bound targets.
- A key component of AMO's integration capabilities, the Air and Marine Operations Center (AMOC) at March, Air Reserve Base in Riverside, California, integrates military and civilian radar tracking data to provide actionable real-time intelligence to AMO aircraft and vessels throughout the Western Hemisphere. Other customers include the National Capital Region Coordination Center (NCRCC), NORAD, the U.S. Secret Service operations center and the Transportation Security Operations Center. The establishment of an additional center with like capabilities on the east coast is being investigated.
- CG is using a risk management system to identify High Interest Vessels for follow-up security boardings and when necessary, due to risk, vessel escorts and positive control boardings to ensure the safety of vessels during their transit into U.S. ports.
- In partnership with the Chief of Naval Operations (CNO), the CG is establishing interagency prototype joint harbor operations centers in select Navy homeports improving both port security and force protection capabilities. Such prototypes are underway in San Diego, California and Hampton Roads, Virginia.
- TSA will soon begin the prototype phase in developing the Transportation Worker Identification Credential (TWIC), aimed at mitigating the threat of attacks to the national transportation infrastructure. The TWIC prototype and supporting measures will test how best to assess the risks of transportation workers entering secure area of our national transportation system. The President's FY 2005 request includes spending authority to begin implementing the TWIC concept within parameters that will be defined by the Administration after completion of the prototype assessment.
- Complementing the TWIC, the CG will continue aggressive implementation of a Merchant Mariner Documentation (MMD) Task Force plan, which ensures positive identity of merchant mariners sailing on U.S. flag vessels and performs appropriate security/background screening. In 2004, the CG will provide for additional personnel support at Regional Examination Centers, centralized security screening and electronic fingerprinting capability.
- The CG has established additional Maritime Intelligence Fusion Centers on the east and west coasts for both military intelligence and law enforcement sensitive information. In addition, the CG established subordinate Field Intelligence Support Teams (FISTs) in key ports. These teams are actively engaged in Intel collection and first order analysis in coordination with federal, state, and local enforcement and Intel agencies. They are "joint" in the broadest sense providing a critical top-down and bottom-up information and intelligence.

- In recognition that the threat in the post-September 11, 2001 strategic environment may seek to avoid hardened legal points of entry by exploiting existing smuggling routes, ICE/AMO marine personnel working closing with ICE Office of Investigations conduct unique undercover and intelligence gathering within high-threat, non-commercial maritime communities and transit areas as well as commercial points of entry.

Aside from the important initiatives above, we are seeing consistent and steady improvements in our ability to integrate and correlate information in the field such that we can effectively respond. For example, on March 13, 2004 the Coast Guard Pacific Area Maritime Intelligence Fusion Center advised CG Marine Safety Office (MSO)/Group Los Angeles/Long Beach that a 728-foot foreign flagged motor vessel with a cargo of crude oil was due into Los Angeles but failed to file an Advance Notice of Arrival properly. The MSO/Group responded and conducted a positive control boarding alongside ICE personnel while the vessel was at anchor. The crew was detained onboard due to improper visas. While we have much more work to do, our maritime domain awareness is improving every day.

Prevention - Create and Oversee Maritime Security Regime

This element of our strategy focuses on both domestic and international efforts and includes initiatives related to MTSA implementation, IMO regulations such as the ISPS Code, as well as improving supply chain security and identity security processes. Recent accomplishments and future plans include:

- The CG has established Area Maritime Security Committees (AMSC), which assist in the development of Area Maritime Security Plans nationwide, as required by the MTSA. AMSCs will enhance maritime situational awareness and ensure integrated maritime prevention and response operations among the entire maritime community. CBP and TSA have designated representatives assigned to the Area Maritime Security Committees to assist CG Captains of the Port in addressing cargo security issues.
- The CG has completed Port Security Assessments (PSA) at 19 of the 55 most significant military and economic ports in the U.S. and will complete the assessments of all 55 strategic ports by the end of calendar year 2004.
- Final CG MTSA implementation Rules, drafted in cooperation with TSA, CBP and the Maritime Administration (MARAD), were published in October 2003 and security plans from approximately 9,500 vessels and 3,500 facilities were due on December 31, 2003. To date, approximately 99% have been received. The CG will continue to aggressively pursue 100% compliance, and has instituted a phased implementation of penalties to ensure that all regulated facilities have implemented approved security plans by the July 1, 2004 deadline.
- The Coast Guard is actively involved with MARAD in the development of maritime security competency standards and security training curricula under Section 109 of MTSA.
- The CG has met with approximately 60 countries representing the vast majority of all shippers to the U.S., reinforcing a commitment to the ISPS code. For vessels subject to MTSA, the Safety of Life at Sea (SOLAS) amendments and the ISPS Code, the CG is implementing strong Port State Control measures to aggressively ensure foreign vessels have approved plans and have implemented adequate security standards. The measures

include tracking performance of all owners, operators, flag administrations, recognized security organizations, charterers, and port facilities. Noncompliance will subject the vessel to a range of control measures, which could include denial of entry into port or significant delay. This aggressive Port State Control regime will be coupled with the CG's inter-agency IPSP, comprised of representatives from the Department of State, Department of Defense, CBP, TSA, and MARAD, that will assess both the effectiveness of anti-terrorism measures in foreign ports and the foreign flag administration's implementation of the SOLAS amendments and the ISPS Code.

- CBP's Container Security Initiative (CSI) enhances the security of ocean-borne container traffic by placing multi-disciplinary CSI teams alongside host government customs officers to ensure that all shipments that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CSI is currently operational at 18 foreign seaports and the program will expand to 17 additional foreign ports in calendar year 2004. Once CSI is fully implemented, nearly 80 percent of all cargo containers headed for the United States will be prescreened prior to lading before they depart from abroad.
- In December 2003, DHS promulgated final regulations implementing the Trade Act of 2002, requiring advance, electronic manifest information for all modes of transportation. This information will augment that received and analyzed already at the National Targeting Center.
 - For vessel operations CBP receives cargo declaration information for all container vessels and non-approved break bulk shipments 24-hours prior to loading the vessel at the foreign port. With the implementation of the Trade Act, CBP now requires this cargo information in an electronic format via the Sea Automated Manifest System (AMS). On March 4, 2004 all container vessels must submit their cargo declaration information to CBP electronically.
 - The Trade Act also provides for all modes of transportation, inbound and outbound, to require cargo information electronically and in advance of arrival. CBP is currently requiring the data electronically inbound for vessel and is expanding the requirement to the inbound air and land modes of transport over the remaining months of 2004. CBP anticipates requiring reporting of electronic outbound data in the beginning of 2005 in cooperation with Census.
- CBP's Customs-Trade Partnership Against Terrorism (C-TPAT). C-TPAT is an innovative government/private sector partnership program that covers all sectors of the international supply chain. The program calls upon the trade community to systematically establish procedures to enhance their existing security practices and those of their business partners involved in their supply chains. C-TPAT strengthens U.S. borders against acts of terrorism while facilitating the legitimate flow of compliant cargo, conveyances and persons. Currently, over 6,200 members of the international community have demonstrated their commitment to security by partnering with CBP through this program.
- Finally, the Border and Transportation Security Directorate is leading a multi-agency working group in efforts both to augment the Department's current cargo supply chain security programs and meet specific requirements under the MTSA to develop a "Secure Systems of Transportation (SST)" and appropriate performance standards for cargo containers. Under this initiative, involved agencies, including TSA, CBP, CG and the

DHS S&T and IAIP Directorates, are reviewing cargo programs, analytic tools, and other relevant resources within the department in order to identify remaining supply chain vulnerabilities and develop strategies to mitigate these vulnerabilities.

- To advance this initiative, BTS expects to be able to harness the results of ongoing test-bed programs that are examining currently available and new technologies and processes to enhance security for global intermodal supply chains and facilitate the flow of commerce. One of these is the Operation Safe Commerce program, an initiative in which DHS, DOT and the Departments of Justice, Commerce and State, are working with business interests, the largest U.S. container load centers and the maritime industry to develop and share best practices for the safe and expeditious movement of containerized cargo. Test results from OSC will also be joined with those obtained by CBP in its testing of various Smart Box technologies within C-TPAT supply chains, and technologies and processes identified by the Science and Technology Directorate's under its recently published Broad Agency Announcement designed to solicit and test new technologies to be applied to container tracking and intrusion detection.

Protection - Increase Operational Presence/Enhance Deterrence

Our collective efforts to increase operational presence in ports and coastal zones will continue to build upon the layered security posture established by the maritime security strategy. These efforts focus not only on adding more people, boats and ships to force structures but making the employment of those resources more effective through the application of technology, information sharing and intelligence support. Recent accomplishments and future plans include:

- CG's Deepwater Program: A multi-year, performance-based acquisition that will replace or modernize 90 Coast Guard cutters, 200 fixed wing aircraft and multi-mission helicopters and the communications equipment, sensors, and logistics systems required to maintain and operate them. Deepwater will greatly improve the Coast Guard's maritime presence starting at America's ports, waterways, and coasts and extending seaward to wherever the Coast Guard needs to be present or to take appropriate maritime action. Deepwater provides the capability to identify, interdict, board, and where warranted seize vessels or people engaged in illegal/terrorist activity at sea or on the ports, waterways, or coast of America. In FY04, the Deepwater Program:
 - o Commences urgent re-engining of Coast Guard's fleet of short-range helicopters to ensure safe and reliable operations;
 - o Accelerates the development of the Fast Response Cutter;
 - o Begins construction of the first National Security Cutter (frigate-size vessel about 425 feet long);
 - o Acquires an additional Maritime Patrol Aircraft (MPA);
 - o Completes design and shipboard integration of Vertical Unmanned Aerial Vehicles (VUAV);
 - o Commences conceptual development of the Offshore Patrol Cutter; and Delivers 4 Short Range Prosecutors (cutter small boats) for use on the 123' Patrol Boat.
- CBP is employing Non-Intrusive Inspection (NII) technology to screen shipments rapidly for anomalies. Deploying NII technology to our land borders and seaports has increased CBP's ability to detect conventional explosives, nuclear weapons, and other terrorist weapons. NII equipment includes large scale x-ray or gamma-ray imaging systems, portal radiation

monitors, and a mixture of portable and handheld technologies to include personal radiation detection devices that greatly reduce the need for costly, time-consuming physical inspection of containers and vehicles.

- CBP currently has 599 Personal Radiation Detectors (PRD) and 60 Radiation Isotope Identifier Devices (RIID) deployed at Border Patrol checkpoints nationwide. Radiation detection equipment is being incorporated into our routine roving patrol duties, marine operations and transportation check assignments, which include airports and train check operations.
- DHS's priority undertaking is preventing weapons of mass destruction from entering this country. The DHS goal is to screen 100% of all arriving containers, trucks, trains, cars, mailbags and express consignment packages with radiation detection equipment. To achieve this goal, CBP has developed a comprehensive risk management strategy for the deployment of radiation portal monitors (RPM) throughout the country.
- As of April 29, 2004, 269 RPMs have been deployed. The vast majority of the deployed RPMs are at International Mail Branches, Express Consignment Courier facilities and along major Northern Border ports of entry. Presently, CBP has begun deployment to our seaports. CBP has also deployed a large number of handheld radiation detection technologies. Currently, CBP has 321 radiation isotope identifier devices and over 9,418 personal radiation detectors to the field.
- Prior to the attacks of 9/11, the CG had committed less than 2% of its assets to active port security duty. Immediately after 9/11, the CG surged nearly 60% of its assets in immediate support of port security. Since then, the CG has rebalanced asset deployments to provide roughly 28% of its assets in coverage of port security –a significant and steady increase in operational presence.
- CG Maritime Safety & Security Teams (MSSTs) provide immediately deployable multiple-boat, law enforcement capability that can be sustained over an extended period. Teams are equipped to deploy (via land or air) to any location within 12 hours of notification. To date, eight of thirteen MSSTs have been commissioned and the remainder will be operational by the end of CY 2004.
- CG is equipping helicopters with Airborne Use of Force (AUF) and Vertical Insertion (VI) capability. This will enhance the Coast Guard's ability to secure our oceans, ports, waterways, and coastal areas against illegal drug, migrant, and terrorist activity by providing capability to fire warning shots and disabling fire and rapidly/covertly deploying boarding teams aboard vessels at sea. The Coast Guard currently has 8-armed MH-68 helicopters operating out of Jacksonville, FL and will equip four HH-60J armed helicopters by April 2004.
- TSA is implementing the "Synergy Project," to test the long-term feasibility of screening and transferring passenger baggage from seaport to airport, reducing the congestion at airport security checkpoints caused by the influx of large number of passengers disembarking from cruise ships. This program is currently underway at the ports of Miami and Vancouver.
- Responding to threat assessments in and in support of the Maritime Homeland Security Strategy, CG Stations Boston and Washington, D.C. were created in Fiscal Year 2004.

Response and Recovery - Improve Response and Recovery Posture

Understanding the challenge of defending 26,000 miles of navigable waterways and 361 ports against every conceivable threat at every possible time, we are also aggressively working to improve our response capabilities and readiness. While the above increases in operational presence necessarily augment our collective response posture, additional accomplishments and future plans include:

- The Secretary announced on March 1, 2004 the approval of the National Incident Management System (NIMS). It is the Nation's first standardized management approach that will provide a consistent nationwide template to enable federal, state, local, and tribal governments as well as private-sector organizations to work together effectively to prepare for, prevent, respond to, and recover from a terrorist attack or other major disaster. NIMS will ensure that all of our nation's responders are working in support of "one plan, one team, one fight." For the first time, there will be standardized procedures for responding to emergencies across the nation. A NIMS Integration Center will also be established to identify and share best practices on preparedness with state and local authorities, provide consistent training to first responders across the country, and conduct exercises involving many different localities.
- Continue deployment of Rescue 21 – the CG's maritime 911 command, control and communications system in our ports, waterways, and coastal areas. Nationwide implementation continues during 2004. This system provides Federal, state and local first responders with interoperable maritime communications capability, greater area coverage, enhanced system reliability, voice recorder replay functionality, and direction finding capability. Rescue 21 represents a quantum leap forward in communications technology.
- ICE AMO has been developing and exercising the capability to deliver via fast rope, incident response teams. This capability will provide AMO the capability to deliver ICE Office of Investigations and Federal Protective Service Critical Response Teams to the scene of incidents with a much shorter response time.
- DHS agencies, including Emergency Preparedness & Response, TSA CG, CBP, and the Office of Domestic Preparedness are working closely with DOT's Maritime Administration (MARAD) and other modal administrations to develop standards and policies to enhance coordination of the recovery of the transportation system in the event of a transportation security incident. For example, TSA is working with MARAD to study the impacts and lessons learned from the recent four-day closing of the Mississippi River caused when a barge sank from hitting the Greenville Bridge linking Mississippi and Arkansas.
- DHS agencies routinely lead or participate in national intermodal terrorism exercises, such as Operation Heartland, United Defense and TOPOFF2, designed to enhance our ability to prevent, mitigate, and respond to potential transportation security incidents.

DHS's response and recovery organization was further strengthened at the "California Spill of National Significance 2004" exercise (CAL SONS 04), which was held 20-24 April 2004. CAL SONS 04 was a CG-sponsored full-scale national exercise that posed two major marine incidents off the coast of Southern California and required a coordinated response by local, state and federal agencies, the government of Mexico, industry partners and volunteer organizations. CAL SONS 04 was guided by the Initial National Response Plan and National Oil and Hazardous Substance Pollution Contingency Plan. It involved the broad range of response and recovery functions including rescue, mobilization of people and resources, multi-level incident

management, tactical operations and testing of industry and agency contingency plans. The CG's National Strike Teams, which have been trained for Chemical, Biological and Radiological responses and were instrumental in the response and recovery operations at the recent Ricin incident in the Senate Office Building, were also deployed. This exercise successfully showed the integration among the various command centers including the Homeland Security Operations Center, the Interagency Incident Management Group, the National Response Team, the Coast Guard Headquarters Crisis Action Center and the local incident command center.

In summary, DHS is taking a comprehensive approach to the needs of maritime security. It cannot start and end at our maritime borders. Rather, it will take an integrated and coordinated approach that stretches from ports such as Miami and Los Angeles to Singapore and Rotterdam.

Service to the Public - Effect on Commerce

In addition to Awareness, Prevention, Protection, Response and Recovery a sixth strategic goal of the Department of Homeland Security is *Service*. In this, we will strive to serve the public effectively by facilitating lawful trade, travel and immigration.

The Department is sensitive to the impact that increased security may have on commerce. The wide variety of security measures implemented to date has had no significant adverse impacts on the flow of maritime commerce. That said, we note that the cost to industry to comply with MTSA regulations is estimated to be \$1.5 billion in the first year and \$7.3 billion over the next 10 years. While we clearly understand that the cost of these security regulations to the maritime industry is not insignificant, a terrorist incident against our marine transportation system could have a devastating and long-lasting impact on global shipping, international trade, and the world economy. A terrorist act that closed a major port could cost up to \$2 billion per day in economic loss to the United States.

The Department understands there will be short-term costs, particularly for many smaller ports or companies with less existing security. Nonetheless, as the industry owns the infrastructure that is being protected, and benefits from that ownership, they should rightly be involved in protecting their infrastructure. We are engaged with the maritime industry to provide information on any available federal funding. Thus far, the Department has awarded or made available a total of nearly \$500 million in port security grants over two years. There is also a shared cost burden by the government. The Department of Homeland Security, and its associated agencies, has spent hundreds of millions of dollars to improve our capability to protect the Marine Transportation System. However, the cost of securing America cannot be left exclusively to the American taxpayer.

In addition, we are continuously seeking out technology and procedural changes that will make our efforts not only more effective and efficient but also less onerous on the vast majority of maritime stakeholders who pose no threat to maritime security. As an example, the CG is incorporating an option in the 96-hour vessel notice of arrival (NOA) requirements to permit electronic submission of information. This e-NOA submission method will allow for importation of data into the CG's National Vessel Movement Center (NVMC) database, the Ship Arrival Notification System (SANS), eliminating all but minimal manual data entry. This will significantly enhance the processing and identification of security and safety risks posed by vessels entering our ports and move information to the field much more rapidly. By merging CBP and CG vessel and people information requirements into the e-NOA, the reporting burden on the maritime industry will be reduced. When the e-NOA system is fully developed, vessel owners and operators will have the option to use the e-NOA to satisfy CBP's Advance Passenger Information Service (APIS) requirements as well as the CG's NOA requirements.

The security requirements of the MTSA were developed with the full cooperation of the private sector. We have developed the security regulations to be performance-based, providing the majority of owners and operators with the flexibility to implement the most cost-effective operational controls, rather than more costly physical improvement alternatives. By establishing consistent national and international security requirements we will also be helping businesses by leveling the playing field. Consistency helps business – consistency amongst companies, states and countries. The Department will be vigilant in its Maritime Homeland Security mission and will remain sensitive to the impact of security measures on maritime commerce.

Conclusion

Our maritime security is first and foremost about awareness – gathering and synthesizing large amounts of information and specific data from many disparate sources to gain knowledge of the entire domain. Maritime Domain Awareness and the knowledge it imparts will allow maritime law enforcement and regulatory agencies to respond with measured and appropriate action to meet any threat. However, it will require the continued growth and development of strong partnerships not the least of which is among the CG, TSA, ICE and CBP, state and local agencies and our collective maritime stakeholders. No single maritime stakeholder whether it is government, industry, or private sector can do this alone. We must continue to work together to improve security. This is never more important than now in our collective national imperative to defend our nation and win the war against terrorism.

The men and women of DHS have accomplished a great deal in the past year and we are each very proud of them. In the end, no amount of planning or strategizing is worth the paper it is written on without the dedicated effort of committed men and women who wake up every day with the safety and security of their nation on their minds. Thank you for the opportunity to testify before you today. We will be happy to answer any questions you may have.